ANSSI | Agence nationale de la sécurité des systèmes d'information

ACTUALITÉS

LPM 2019 – 2025 : LA PUBLICATION DU DÉCRET D'APPLICATION DE L'ARTICLE 34 RENFORCE LES MISSIONS DE L'ANSSI

La loi n°2018-607 relative à la programmation militaire pour les années 2019 – 2025 a été promulguée par la Président de la République le 13 juillet 2018. Elle comporte, dans son article 34, des dispositions relatives au renforcement des capacités de détection des attaques informatiques, aujourd'hui indispensables pour élever le niveau de sécurité de la Nation. Le décret d'application publié au journal officiel aujourd'hui vient en préciser les modalités de mise en application, avec une entrée en vigueur au 1er janvier 2019.

Pour répondre à l'accroissement du niveau général de la menace, le renforcement de la capacité nationale de détection, de caractérisation et de prévention des attaques informatiques apparaît comme prioritaire.

Confortant le modèle français en matière de cyberdéfense, l'article 34 de la loi n°2018-607 relative à la programmation militaire pour les années 2019 – 2025 ↗, et son décret d'application ↗ viennent aujourd'hui renforcer les missions de l'ANSSI en améliorant ses capacités de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, des autorités publiques et d'opérateurs publics et privés ↗. Ce cadre législatif s'inscrit dans une démarche vertueuse et de confiance, visant à élever significativement le niveau de sécurité global de la France en collaboration étroite avec les opérateurs de communications électroniques et les hébergeurs.

IMPLICATION DES OPÉRATEURS DE COMMUNICATIONS ÉLECTRONIQUES POUR ÉLEVER LE NIVEAU DE CYBERSÉCURITÉ

Le premier volet de l'article 34 permet aux opérateurs de communications électroniques (OCE) de mettre en œuvre des dispositifs de détection d'attaques informatiques affectant les systèmes d'information de leurs abonnés, pour mieux les en informer le cas échéant.

Si une attaque détectée concerne un opérateur d'importance vitale, un opérateur de services essentiels ou une autorité publique, l'ANSSI pourra demander des informations techniques complémentaires pour caractériser l'attaque et établir des mesures de protection et de remédiation adaptées avec la victime.

DÉPLOIEMENT DE DISPOSITIFS DE DÉTECTION

Afin de caractériser une menace informatique et d'en prévenir les conséquences pour de potentielles victimes, il est souvent précieux de pouvoir procéder à des opérations techniques permettant d'observer et d'analyser le mode opératoire d'un attaquant.

Le second volet du dispositif donne ainsi la possibilité à l'ANSSI, lorsqu'elle a connaissance d'une menace grave et imminente sur les systèmes d'une autorité publique, d'un OIV ↗ ou d'un OSE ↗ , de mettre en place un dispositif de détection local et temporaire sur un serveur d'un hébergeur ou un équipement d'un opérateur de communications électroniques contrôlé par un attaquant. Le dispositif de détection est mis en œuvre pour une durée et sur un périmètre limités, strictement nécessaires à la caractérisation de la menace.

CONTRÔLE DE L'ARCEP

Le respect du cadre juridique dans lequel s'inscrivent les nouvelles missions de l'ANSSI est placé sous le contrôle d'une autorité administrative indépendante, l'Autorité de régulation des communications électroniques et des postes (ARCEP). Le décret précise les modalités de l'exercice de ce contrôle.